DOI:10.16749/j.cnki.jecjtu.2014.02.018

文章编号:1005-0523(2014)02-0095-04

基于ECC和指纹USBKey的身份认证协议

张利华,沈友进

(华东交通大学电气与电子工程学院,江西 南昌 330013)

摘要:分析了现有网络身份认证方案的不足,给出了一种指纹识别技术与USBKey技术相结合的身份认证方案。利用载有指纹特征的指纹USBKey改进现有的USBKey认证技术。利用椭圆曲线密码算法ECC(elliptic curve cryption),提高身份认证协议的安全性。采用挑战与应答的认证机制,实现了双向身份认证。使用含指纹特征的数字证书,防止非法用户篡改指纹特征。给出的身份认证协议实现了USBKey对用户权限的验证及远程服务器对用户身份的实体认证。能够有效抵御窃听攻击、假冒攻击、重放攻击及DoS攻击。

关键词:身份认证;USBKey;指纹;椭圆曲线密码算法

中图分类号:TP309 **文献标志码**:A

远程身份认证是保障网络安全的重要手段。常见的身份认证方式有静态口令认证、动态口令认证、智能卡认证、USBKey认证及生物认证。静态口令认证易遭受口令猜测攻击与字典攻击,且口令明文传输易被窃听[1]。动态口令认证,由于时间漂移的存在导致时间机制的失步和维护事件同步的复杂性[2]。智能卡认证存在智能卡丢失/复制攻击,且智能卡的加解密计算能力有限[3-4]。现有的基于USBKey的身份认证协议,使用PIN码对USBKey的使用权限进行验证,然而一旦用户的PIN码被盗或被木马窃取,则非法入侵者将会轻而易举地控制USBKey进行身份认证[5]。Ge Xiaomin等[6]提出了一种基于指纹特征的身份认证,但是该方案将指纹特征在不安全的网络上传输,这会使得非法入侵者在网络传输过程中,窃取指纹图像,进行重放攻击。为此,学者们提出了一些改进措施,将静态/动态口令认证、智能卡认证、USBKey认证及生物认证等方法融合,形成多因子身份认证,增加身份认证协议的安全性,如文献[7-9],但由于身份认证的复杂性与网络攻击的多样性,简单物理融合的认证方案,并不能完全解决网络身份认证的难题。

针对网络身份认证中存在的问题,提出一种基于ECC(elliptic curve cryptography)密码算法的指纹USBKey身份认证方案。通过将含有指纹特征的数字证书嵌入USBKey,利用指纹代替PIN码验证USBKey的使用权限,且将指纹融入用户远程身份认证。通过ECC对身份认证中的交互信息进行加密,保障数据的传输安全。采用挑战—应答认证机制,融合指纹与USBKey身份认证技术,实现双因子的双向认证,提高网络身份认证的安全性。

1 ECC密码算法和指纹USBKey技术

ECC是一种基于椭圆曲线离散对数难题的密码算法,比传统的对称密码算法AES安全性高[10]。比目前使用广泛的基于大数因式分解难题的RSA密码算法,有着明显的安全优势,并且在同等的安全保密能力下,ECC的密钥长度比RSA密钥长度要小得多,从而运算速度更快、效率更高。ECC密码算法是利用椭圆曲线 $E(F_q)(q>3)$ 上阶为 n 的基点 G,选择私钥 $x(x<n)$,计算公钥 $K=xG$。利用公私钥对可进行加解密签名

收稿日期:2013-11-06

基金项目:国家863计划项目(2006AA04A134)

作者简介:张利华(1972—),男,副教授,博士,主要研究方向为电气信息技术,通信网络信息安全。

运算。

指纹USBKey身份认证方案，是将ECC密码算法、指纹识别技术与USBKey技术相结合，构造新型的指纹USBKey。指纹USBKey是一种集指纹传感器、指纹处理芯片、信息安全芯片、内嵌COS（chip operation system）等的USB接口设备。指纹传感器与指纹处理芯片构成指纹USBKey的指纹处理模块，信息安全芯片及内嵌COS构成信息安全模块，其结构如图1所示。

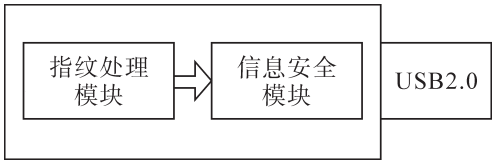

图1 指纹USBKey

Fig.1 Fingerprint USBKey

指纹USBKey内置ECC加密签名算法，存储含指纹特征的数字证书、用户信息及用户私钥。指纹USBKey可用于数字签名与加解密计算。由于指纹USBKey存储的私钥保存于USBKey密钥存储区内，不能导出USBKey，所有的加解密签名运算都在USBKey中进行，保证了私钥的安全。

利用指纹特征改进传统USBKey采用PIN码保护的方式，防止PIN码被盗或被木马窃取，使得USBKey与用户实体身份构成一一对应关系，实现USBKey对用户的实体验证。并且利用含指纹特征的数字证书证书，实现远程服务端对用户的实体认证。

为了使用户的指纹特征不被篡改或复制，USBKey的公钥与持有者身份绑定，需通过可信认证中心生成含纹特征的数字证书。在USBKey初始化时，将数字证书固化在USBKey中。含指纹特征的数字证书含有用户某手指的指纹特征（记为Mark），指纹特征Mark既用于USBKey使用权限的验证，又用于远程身份认证，具体作用流程如下：

1）指纹特征代替PIN码，实现USBKey对用户的实体身份验证。每当用户使用USBKey时，用户必先输入指纹，利用指纹处理芯片生成指纹特征，与指纹特征Mark进行匹配。特征匹配成功后，用户才有USBKey的使用权限。

2）利用指纹特征证书，实现远程服务端对用户的实体认证。当且仅当用户获得USBKey的使用权限，USBKey才释放与指纹特征证书相对应的指纹特征序列号f_{id}，用于远程身份认证。

2 远程身份认证协议

远程身份认证的主体包括用户（记为User）、指纹USBKey及远程服务端的访问控制中心（记为AS）。AS负责用户注册、证书签发、以及对用户进行身份认证。只有通过身份认证的用户，才能访问服务器端。本协议包括用户注册申请阶段与身份认证阶段。

2.1 用户注册申请阶段

假设AS在ECC密码算法下，输出其密钥对（x_{as}，K_{as}），并公开公钥K_{as}、单向强安全Hash函数$h(\cdot)$。所有注册用户均可获得K_{as}及$h(\cdot)$。AS维护由USBKey唯一序列号Num_x组成的USBKey序列表U_x。

1）USBKey利用内置的ECC密码算法，生成一对密钥（x_u，K_u），并将私钥x_u保存在USBKey中的私钥存储区，私钥将无法改写或导出USBKey。User利用指纹USBKey输入指纹图像，并提取指纹特征$Mark$。USBKey计算 $C_1 = E_{K_{as}}[h(Mark)||Mark]||K_u||Num_i||h(x_u)$ ，其中Num_i为USBKey的唯一序列号。USBKey将C_1发送至AS。

2）AS接收到C_1后，利用其私钥解密C_1，验证Num_i的真实性，若Num_i不属于某个USBKey序列表U_i，则终止注册。若Num_i真实合法，则AS颁发由Mark、指纹序列号f_{id}、K_u、Num_i及AS的数字签名$Sing_{as}$组成的数字证书，即 $Cert_i = E_{K_u}[Mark||f_{id}]||K_u||Num_i||Sing_{as}$ 。AS将$h(f_{id})$、$h(x_u)$及$Cert_i$添加到序列表U_i中，作为用户标识。为了对指纹序列号f_{id}的安全保密，AS销毁f_{id}。最后AS将$Cert_i$发送给用户的USBKey。USBKey将$Cert_i$下载

至USBKey的数字证书存储区。注册阶段完成。

2.2　远程身份认证阶段

远程身份认证具体过程如下：

1）User请求接入服务器端时，将指纹USBKey插入PC机的USB接口，并利用USBKey的指纹传感器，输入指纹图像。USBKey获取用户的指纹特征，与$Cert_i$中的指纹特征模板Mark比较，若指纹特征不一致，则终止身份认证。否则用户取得该指纹USBKey的使用权，用于远程身份认证。用户取得USBKey的使用权后，USBKey计算$C_2=E_{K_{as}}\{E_{x_u}[Num_i,n]\}||Num_i$，其中n为随机数。USBKey将$C_2$发送给AS。

2）AS接收到C_2后，利用Num_i，查找到User的序列表U_i，获取User的公钥K_u，并利用自己的私钥x_{as}解密C_2。得到随机数n，计算$C_3=E_{Ku}\{E_{x_{as}}[h(x_u)||n||c]\}$，其中$c$为与$n$不同的随机数。AS将$C_3$发送给USBKey。

3）指纹USBKey接收到C_3后，利用自己的私钥x_u及AS的公钥K_{as}解密C_3，得到$h'(x_u)$、n'及c。USBKey验证$h'(x_u)$是否等于$H=h(x_u)$，n'是否等于n，若两者验证不都相等，则AS未通过身份认证，终止此次身份认证。否则AS通过身份认证，USBKey计算$C_4=E_{K_{as}}[h(f_{id})||c||r]||Num_i$（其中$r$为不同于$c$的随机数），将$C_4$发送给AS。

4）AS接收到C_4后，利用自己的私钥x_{as}解密C_4，得到$h'(f_{id})$、c'及r。验证$h'(f_{id})$是否等于$h(f_{id})$，验证c'是否等于c，若两者验证不都相等，则指纹USBKey未通过身份认证，即用户User未通过身份认证。否则指纹USBKey通过身份认证，即用户通过身份认证。至此，实现了双向身份认证，本次身份认证过程结束。

3　安全性分析

1）抗窃听攻击。假设攻击者C监听USBKey与AS的认证信息。在远程身份认证阶段的过程1）和3）中，攻击者监听到$C_2=E_{K_{as}}\{E_{x_u}[Num_i,n]\}||Num_i$或$C_4=E_{K_{as}}[h(f_{id})||c||r]||Num_i$，但由于$C$缺乏AS的私钥$x_{as}$，所以根本无法进行解密运算，无法进行攻击。在认证阶段2）中，攻击者C监听到$C_3=E_{Ku}\{E_{x_{as}}[h(x_u)||n||c]\}$，但由于$C$缺乏指纹USBKey的私钥$x_u$，根本无法进行解密运算，所以攻击者$C$无法达到窃听攻击的目的。

2）抗重放攻击。由于指纹USBKey与AS进行身份认证时，认证信息都使用了随机数，保证了信息的新鲜性，攻击者无法进行重放攻击，当攻击者获取到C_2、C_3或C_4后，进行重放时，由于C_2、C_3及C_4都插入随机数，收到消息的认证主体对随机数进行验证判定，使得该攻击方式无效。

3）抗假冒攻击。攻击者C在指纹USBKey与AS的身份认证中，假冒认证实体USBKey或AS，但由于攻击者C没有认证双方的私钥，所以无法进行假冒攻击进行身份认证。当攻击者C假冒指纹USBKey时，发起与AS的身份认证，由于C无User的指纹，则无法使用指纹USBKey，更无法使用指纹特征完成与AS的身份认证。当攻击者假冒AS时，可以获取$C_2=E_{K_{as}}\{E_{x_u}[Num_i,n]\}||Num_i$，但由于没有AS的私钥，也无法得到$n$，更无法利用$n$进行身份认证。

4）抗Dos攻击。在认证阶段过程1）中，所有发向AS的认证请求，必须包含正确的指纹USBKey序列号Num_i及正确的私钥x_u对n的加密，否则AS拒绝本次认证会话，有效抵御Dos攻击。同样，在认证过程4）中，AS接收到$C_4=E_{K_{as}}[h(f_{id})||c||r]||Num_i$，只有解密出的$C_4$含有正确的$h(f_{id})$及随机数$c$，AS才认证User合法，通过身份认证，否则立即关闭认证会话，抵御DoS攻击。

4　结束语

将指纹识别技术与USBKey技术相结合，利用ECC密码算法对认证信息进行加密，构造含指纹特征的数字证书存储在USBKey中，形成双因子身份认证，解决了现有身份认证方案存在的缺陷。利用挑战与应答的认证机制，实现用户与服务器端的双向认证。指纹特征代替USBKey的PIN码能有效抵御因PIN被盗带来的口令攻击行为，实现了USBKey对用户的验证。利用指纹特征序列号f_{id}避免了指纹特征直接在开放

的网络中直接传输带来的安全威胁,实现了远程服务端对用户的生物认证。指纹USBKey存储用户私钥,保障了用户私钥的安全性。构建含指纹特征的数字证书,能防止攻击者篡改USBKey中的指纹特征进行假冒攻击。经安全性分析,本方案有较高的安全性。

参考文献:

[1] 方恩博,刘嘉勇,肖丰霞. 一种适于受限资源环境的远程用户双向身份鉴别方案[J]. 四川大学学报: 工程科学版, 2011,43(5):140-145.

[2] 刘潇,刘巍然,李为宇. 一种改进的动态口令生成算法及重同步方案[J]. 计算机研究与发展,2012,49(12):2611-2618.

[3] LI CHUNTA, HWANG MINSHIANG. An efficient biometrics-based remote user authentication scheme using smart cards[J]. Journal of Network and Computer Applications,2010(33):1-5.

[4] 余卿斐,杨晓元,周宣武. 基于ECC的远程用户智能卡认证方案[J]. 计算机工程,2009,35(5):142-143.

[5] 陈学礼,冯姝雯. 基于USBKEY的身份管理与认证系统的研究及实施[J]. 信息系统工程,2013,20(1):74.

[6] GE XIAOMIN,WU CUIHONG. Analysis and research for multi-mode identity authentication of E-commerce [C]// Proceedings of 2010 The 3rd International Conference on Computational Intelligence and Industrial Application,Wuhan: Springer-Verlag, 2011:507-513.

[7] 刘怀兰,侯昕,王佳. 改进的基于USBKey的动态身份认证方案[J]. 华中科技大学学报,2010,38(11):41-43.

[8] 郑建德,郑杭杰,杨静. 一种口令、令牌与生物认证技术通用集成框架[J]. 厦门大学学报:自然科学版,2011,50(1):42-46.

[9] 黄朝阳. 基于指纹和智能卡的PKI双向认证系统[J]. 计算机系统应用,2012,21(10):198-200.

[10] 殷爱菡,王胜凯. 基于改进的AES算法的EPON安全方案研究[J]. 华东交通大学学报,2013,30(4):35-39.

A Novel User Authentication Scheme Based on ECC and Fingerprint USBKey

Zhang Lihua,Shen Youjin

(School of Electrical and Electronic Engineering, East China Jiaotong University, Nanchang 330013, China)

Abstract: Network user authentication schemes are analyzed in this paper, and then a new authentication model combining the fingerprint recognition technology with USBKey technology is proposed, which uses fingerprint USBKey with fingerprint characteristics to improve the existing USBKey authentication. The ECC (Elliptic Curve Cryptography) algorithm is utilized to improve the security of user authentication protocol. The challenge/response authentication mechanism is adopted to achieve the mutual authentication. The digital certificate with fingerprint characteristic is exploited to prevent unauthorized users from tampering with fingerprint characteristics. The user authentication scheme presented in this paper may judge the user authority by USBKey, realize the remote server authentication, and effectively resist the eavesdropping attack, impersonation attack, replay attack and DoS attack as well.

Key words: user authentication; USBKey; fingerprint; ECC (elliptic curve cryptography) algorithm